CLAIMS

1. A method for providing an application credential to an application running on a device, wherein the application credential is used by the application to authenticate to a data server, the method comprising:

receiving a request to generate the application credential, wherein the request includes an application identifier; and

generating the application credential using the application identifier and a master credential associated with the device.

2. The method of claim 1, wherein the step of generating the application credential comprises a one-way generation technique, so that the application identifier and the master credential can not be discovered from the application credential.

3. The method of claim 1, further comprising using a modification detection and authentication technique to determine if the application or the application identifier has been modified and prove the application is associated with the application identifier

4. The method of claim 3, wherein the modification detection technique is generated by a server that is distinct from a provider of the application.

5. The method of claim 4, wherein the modification detection technique is a digital signature.

6. The method of claim 1, wherein the device is a wireless device.

7. Apparatus that operates to provide an application credential to an application running on the device, wherein the application credential is used by the application to authenticate to a data server, the apparatus comprising:

receiving logic that operates to receive a request for the application credential, wherein the request includes an application identifier; and

generating logic that operates to generate the application credential using the application identifier and a master credential.

8. The apparatus of claim 7, wherein the generating logic uses a one-way credential generation technique, so that the application identifier and the master credential cannot be discovered from the application credential.

9. The apparatus of claim 8, further comprising a modification detection and authentication technique that operates to determine if the application or the application identifier have been modified and prove the application is associated with the application identifier.

10. The apparatus of claim 9, wherein the modification detection technique is generated by a server distinct from a provider of the application.

11. The apparatus of claim 10, wherein the modification detection technique is a digital signature.

12. The apparatus of claim 7, wherein the device is a wireless device.

13. Apparatus that operates to provide an application credential to an application running on the device, wherein the application credential is used by the application to authenticate to a data server, the apparatus comprising:

means for receiving a request for the application credential, wherein the request includes an application identifier; and

means for generating the application credential using the application identifier and a master credential.

14. The apparatus of claim 13, further comprising means for generating the application credential using a one-way generation technique, so that the application identifier and the master credential cannot be discovered from the application credential.

15. The apparatus of claim 13, further comprising means for using a modification detection and authentication technique to determine if the application or application identifier have been modified and prove the application is associated with the application identifier.

16. The apparatus of claim 15, wherein the modification detection technique is generated by a server distinct from a provider of the application.

17. The apparatus of claim 16, wherein the modification detection technique is a digital signature.

18. A computer-readable media comprising instructions, which when executed by a processor in a device, provide an application credential to an application running on the device, wherein the application credential is used by the application to authenticate to a data server, the computer readable media comprising:

instructions for receiving a request for the application credential, wherein the request includes an application identifier; and

instructions for generating the application credential using the application identifier and a master credential.

19. The computer-readable media of claim 18, comprising instructions for using a modification detection and authentication technique to determine if the application or the application identifier has been modified and prove the application is associated with the application identifier

20. The computer-readable media of claim 19, wherein the modification detection technique is generated by a server that is distinct from a provider of the application.

21. The computer-readable media of claim 20, wherein the modification detection technique is a digital signature.

22. The computer-readable media of claim 18, further comprising instructions for generating the application credential using a one-way generation technique, so that the application identifier and the master credential cannot be discovered from the application credential.

23. The computer-readable media of claim 18, wherein the device is a wireless device.

24. A method for operating a credential server to authenticate an application running on a device, wherein the application transmits a request for data to a data server and the request comprises an application credential, the method comprising:

receiving an application identifier in a request for a server credential;

generating the server credential using the application identifier and a master credential; and

transmitting the server credential to the data server, wherein if the server credential and the application credential match, the application is authenticated.

25. The method of claim 24, further comprising receiving an authentication token that proves the request is associated with the application identifier.

26. The method of claim 24, further comprising:

receiving the application credential;

matching the application credential and the server credential; and

transmitting an authorization to the data server to fulfill the data request if the application credential matches the server credential.

27. The method of claim 24, wherein the step of generating comprises generating the server credential using a one-way generation technique, so that the application identifier and the master credential cannot be discovered from the server credential.

28. Apparatus for use with a credential server to authenticate an application running on a device, wherein the application transmits a request for data to a data server and the request comprises an application credential, the apparatus comprising:

first receiving logic that operates to receive an application identifier in a request for a server credential;

generating logic that operates to generate the server credential based on the application identifier and a master credential; and

transmitting logic that operates to transmit the server credential to the data server, wherein the data server matches the server credential to the application credential to authenticate the application.

29. The apparatus of claim 28, further comprising receiving an authentication token that proves the request is associated with the application identifier.

30. The apparatus of claim 28, wherein the generating logic comprises logic to generate the server credential using a one-way generation technique, so that the

application identifier and the master credential cannot be discovered from the server credential.

31. The apparatus of claim 28, further comprising:

second receiving logic that operates to receive the application credential; and

matching logic that operates to match the application credential with the server credential, and transmit an authorization to fulfill the data request to the data server if the application credential matches the server credential.

32. Apparatus for use with a credential server to authenticate an application running on a device, wherein the application transmits a request for data to a data server and the request comprises an application credential, the apparatus comprising:

means for receiving an application identifier in a request for a server credential;

means for generating the server credential based on the application identifier and a master credential; and

means for transmitting the server credential to the data server, wherein the data server matches the server credential to the application credential to authenticate the application.

33. The apparatus of claim 32, further comprising receiving an authentication token that proves the request is associated with the application identifier.

34. The apparatus of claim 32, wherein the means for generating comprises means for generating the server credential using a one-way generation technique, so that the application identifier and the master credential cannot be discovered from the server credential.

35. The apparatus of claim 32, further comprising:

means for receiving the application credential; and

means for matching the application credential with the server credential; and

means for transmitting an authorization to fulfill the data request to the data server if the application credential matches the server credential.

36. A computer-readable media comprising instructions, which when executed by a processor in a credential server, operate to authenticate an application running on a device, wherein the application transmits a request for data to a data server

and the request comprises an application credential, the computer-readable media comprising:

instructions for receiving the application identifier in a request for a server credential;

instructions for generating the server credential based on the application identifier and a master credential; and

instructions for transmitting the server credential to the data server, wherein the data server matches the server credential to the application credential to authenticate the application.

37. The computer-readable media of claim 36, further comprising receiving an authentication token that proves the request is associated with the application identifier.

38. The computer-readable media of claim 36, wherein the instructions for generating comprises instructions for generating the server credential using a one-way generation technique, so that the application identifier and the master credential cannot be discovered from the server credential.

39. The computer-readable media of claim 36, further comprising:

instructions for receiving the application credential; and

instructions for matching the application credential with the server credential; and

instructions for transmitting an authorization to fulfill the data request to the data server if the application credential matches the server credential.

40. A method for processing an application credential associated with an application running on a device, wherein the application credential is used by the application to authenticate to a data server, the method comprising:

receiving a request to generate the application credential, wherein the request includes an application identifier;

generating the application credential using the application identifier and a master credential;

transmitting a request for data to a data server, wherein the request comprises the application credential;

requesting a server credential from a credential server, wherein the request for the server credential comprises the application identifier and a token by which the data server authenticates itself;

generating the server credential using the application identifier and the master credential;

transmitting the server credential to the data server;

matching the server credential with the application credential, wherein the application is authenticated if the two credentials match; and

transmitting the data to the application.

41. The method of claim 40, wherein the application credential and the server credential are generated using a one-way generation technique, so that the application identifier and the master credential cannot be discovered.

42. The method of claim 40, further compromising using a modification and authentication technique to determine if the application identifier has been modified and prove the application is associated with the application identifier.

43. The method of claim 42, wherein the modification detection technique is a digital signature.

44. The method of claim 40, further comprising receiving an authentication token at the credential server that proves the request is associated with the application identifier.

45. The method of claim 40, wherein the device is a wireless device.